CENTER FOR ADVANCED AVIATION SYSTEM DEVELOPMENT (CAASD)

Information Security for the Aviation Community: A Personal Perspective

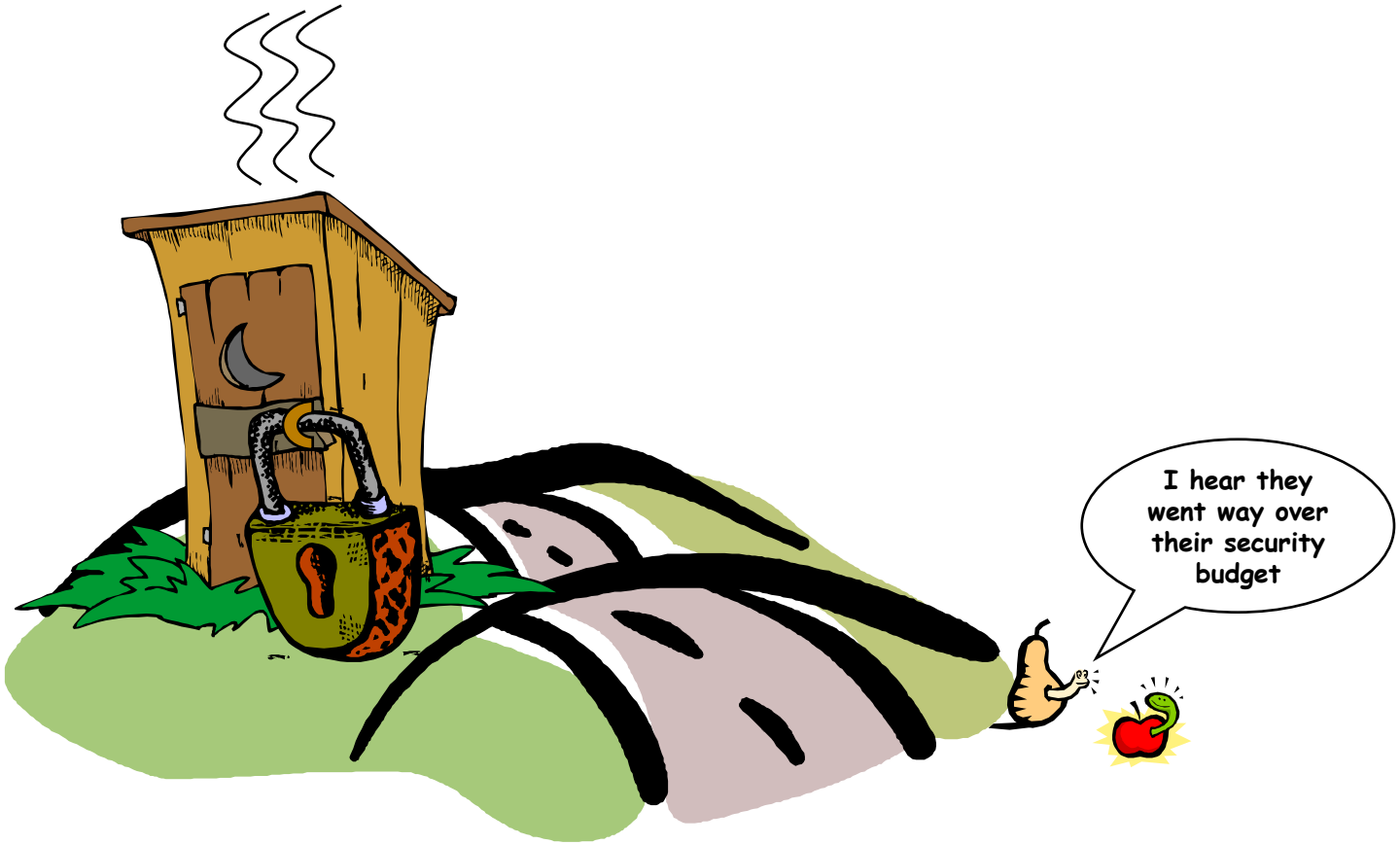
Ted Signore

5/2/05

CAASD

MITRE

Security is Not an Add-on



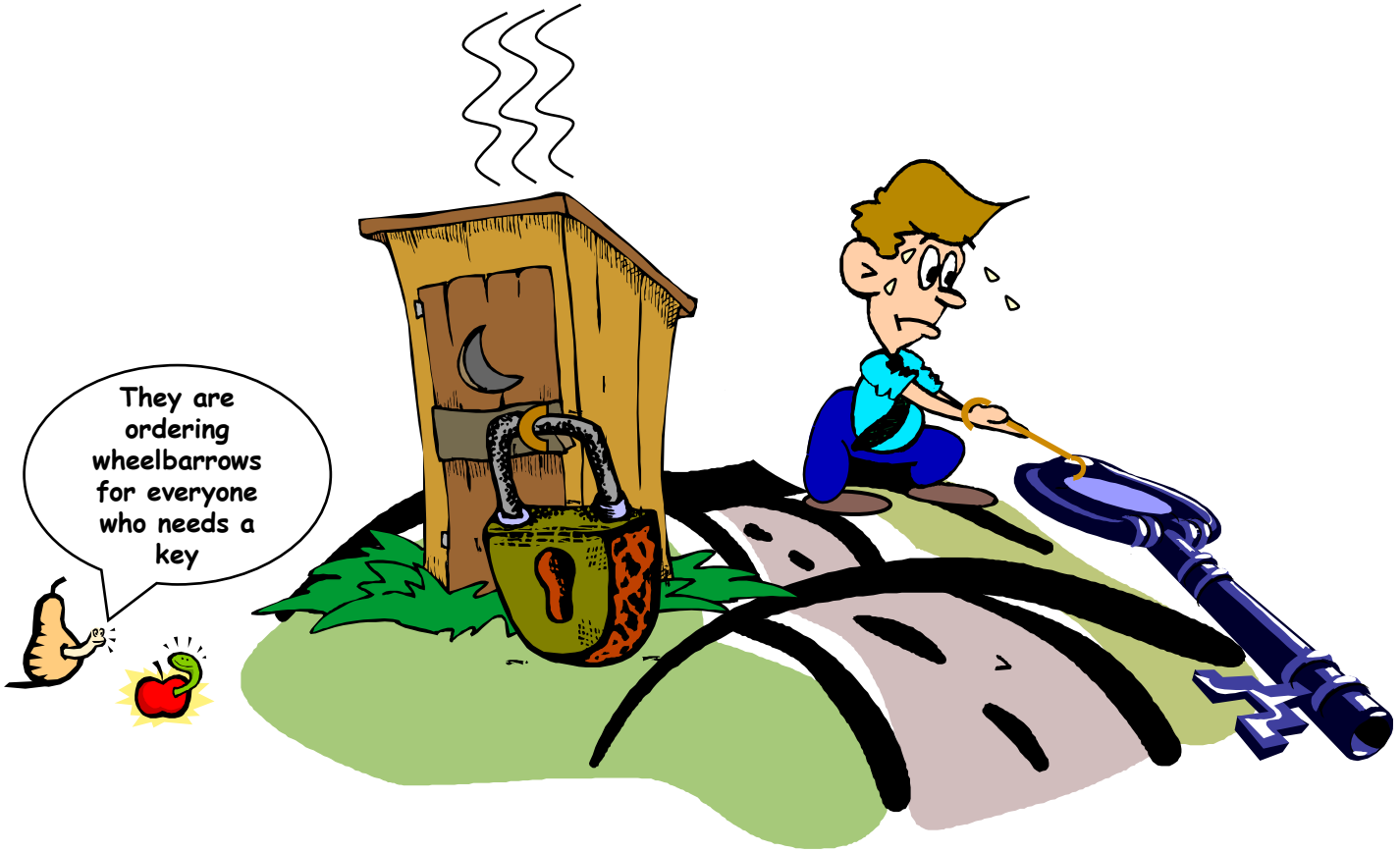
MITRE

Security is Not an Add-on

- Security should be a part of the system design from the beginning
  - You don't design the system, then add security
- Example: Build service, then add Demilitarized Zone (DMZ) for security
  - May need redundant DMZ in safety environment
    - Which DMZ to be used and how?
    - Internal servers may need to support servers in both DMZs
  - Internal servers may need to pull, not push data from DMZ
  - DMZ may prevent remote maintenance by contractor

MITRE

You Have No Security Solution without a Concept of Operations



MITRE

You Have No Security Solution without a Concept of Operations

- Effective security includes management, operational, and technical consideration
  - The technical solution is not the entire answer
- Example: Public/private key solutions
  - Require users to have their public/private key pair plus public keys of users to be contacted
  - Management of keys bigger problem than using the keys
    - Distribute keys, update keys, revoke keys
- Answers to security management issues are critical in a safety related, time critical environment

Security Solution Must Fit Context of Entire System

MITRE

Security Solution Must Fit Context of Entire System

- Aviation services exist within a larger community
- No matter how well your service is protected from INFOSEC threats, your service may be rejected for inclusion into the larger community
  - Because it increases the threat to the entire community
  - Example: Your service uses IPSEC confidentiality and authentication options for all access
    - Does not allow “community” DMZ to examine data

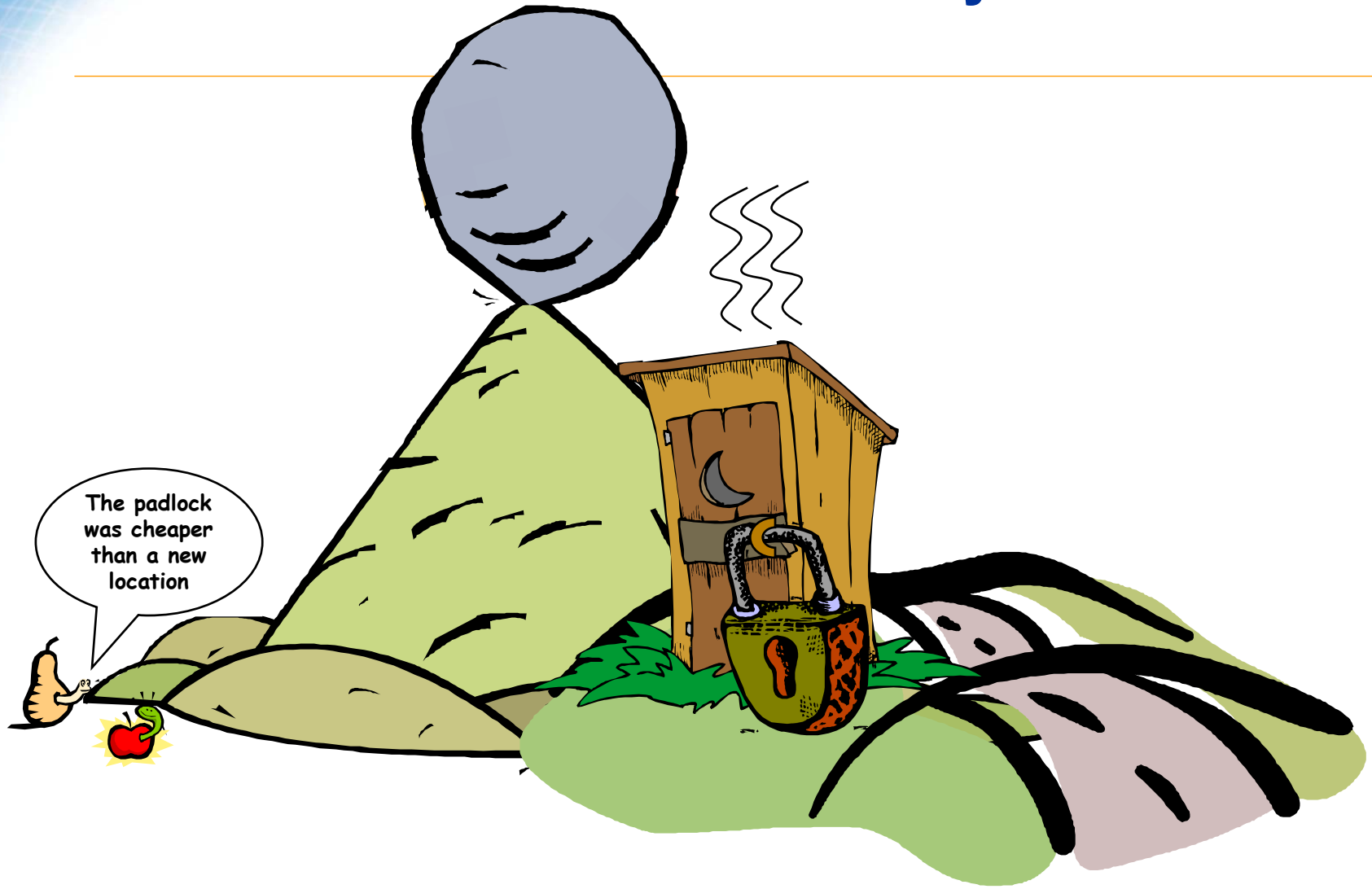
MITRE

What Happens if the Security Solution Fails?

- Safety critical systems may need to continue to operate when components fail, including security
  - Security solutions normally fail in inoperative mode
  - Example: No public key, no communication with others
- Is inoperative failure viable in an aviation system?
  - Example: Air/ground communication must be maintained even if air/ground security solution fails (benign or malicious)
  - If you fail in operative mode, do you need security?
- How do you recover from security failure?
  - Must provide for restoration of service, removal of viruses, replacement of keys
  - Restoration of service must occur in a secure manner

MITRE

Beware Threat Analyses



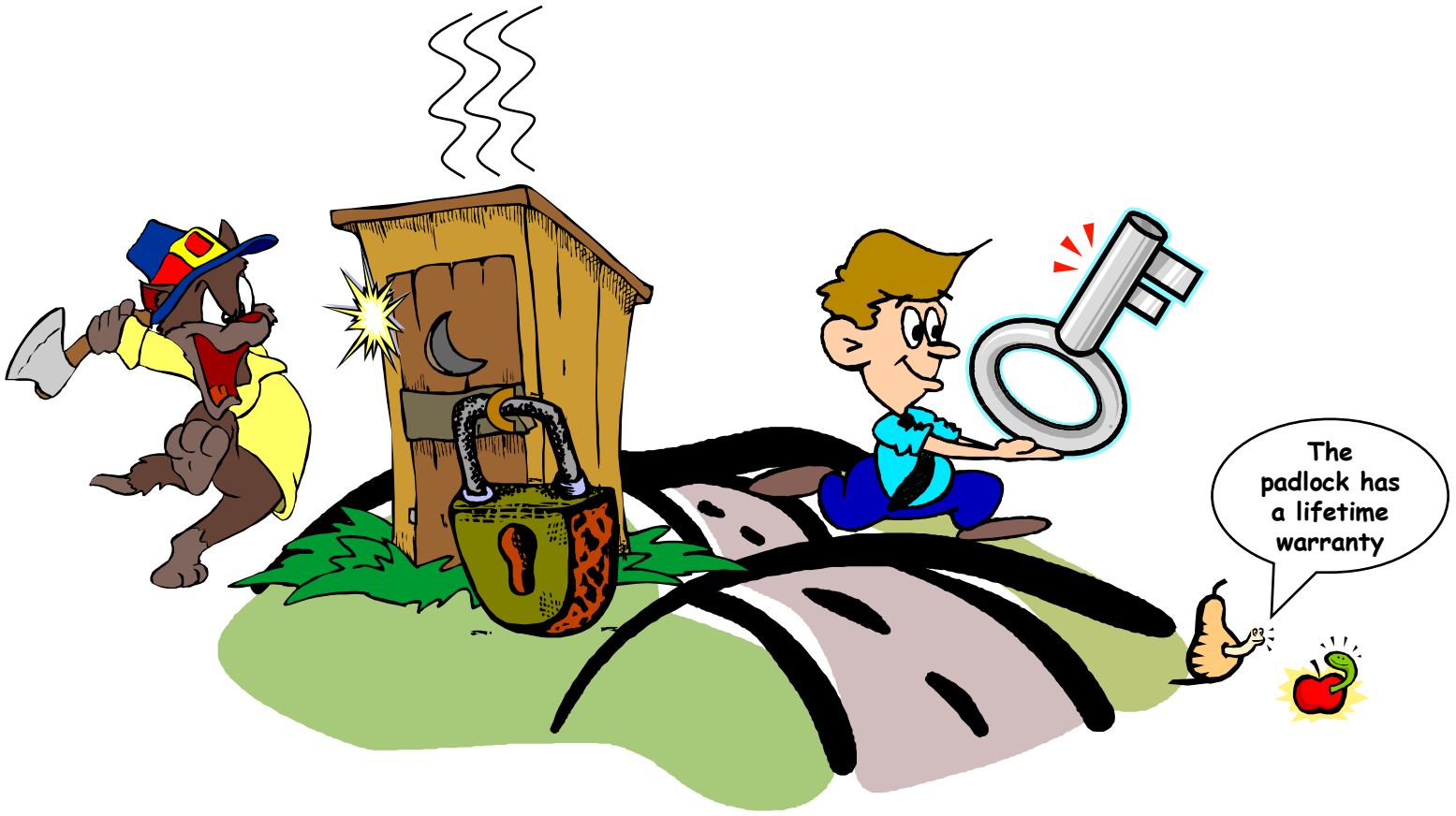
MITRE

Beware Threat Analyses

- "Classical" INFOSEC analysis (e.g., NIST 800-12) may not be useful
  - Determine threat, identify vulnerability, classify risk
- Threats are difficult to define
  - Represent old threats, not new ones
  - Can't include what you haven't thought of
  - Not specific enough to determine security needs
  - Example: How does specific threat of Osama Bin Laden translate into an INFOSEC requirement for your system?
- Better solution
  - Examine risks, address those with worst impact (e.g., FIPS 199)

MITRE

Make Sure the INFOSEC Product Applies to Your Environment



MITRE

Make Sure the INFOSEC Product Applies to Your Environment

- No INFOSEC product is 100% effective
- COTS INFOSEC products are designed to minimize financial loss, not maximize safety
- Example: Firewall
  - Firewall cannot prevent all Denial of Service attacks
    - Firewalls are not the total security answer for publicly accessible server
  - Firewalls need latest signature updates to work
    - No way of quickly updating firewalls means reduced security
- Example: IDS Tool
  - Requires frequent examination of logs to be useful
    - No staff power means no IDS power
- Example: Authentication
  - In a tactical environment delay critical
- Safety related environment may negate usefulness of INFOSEC product

MITRE

Establishing Trust and Identification Is Not in Itself a Security Solution

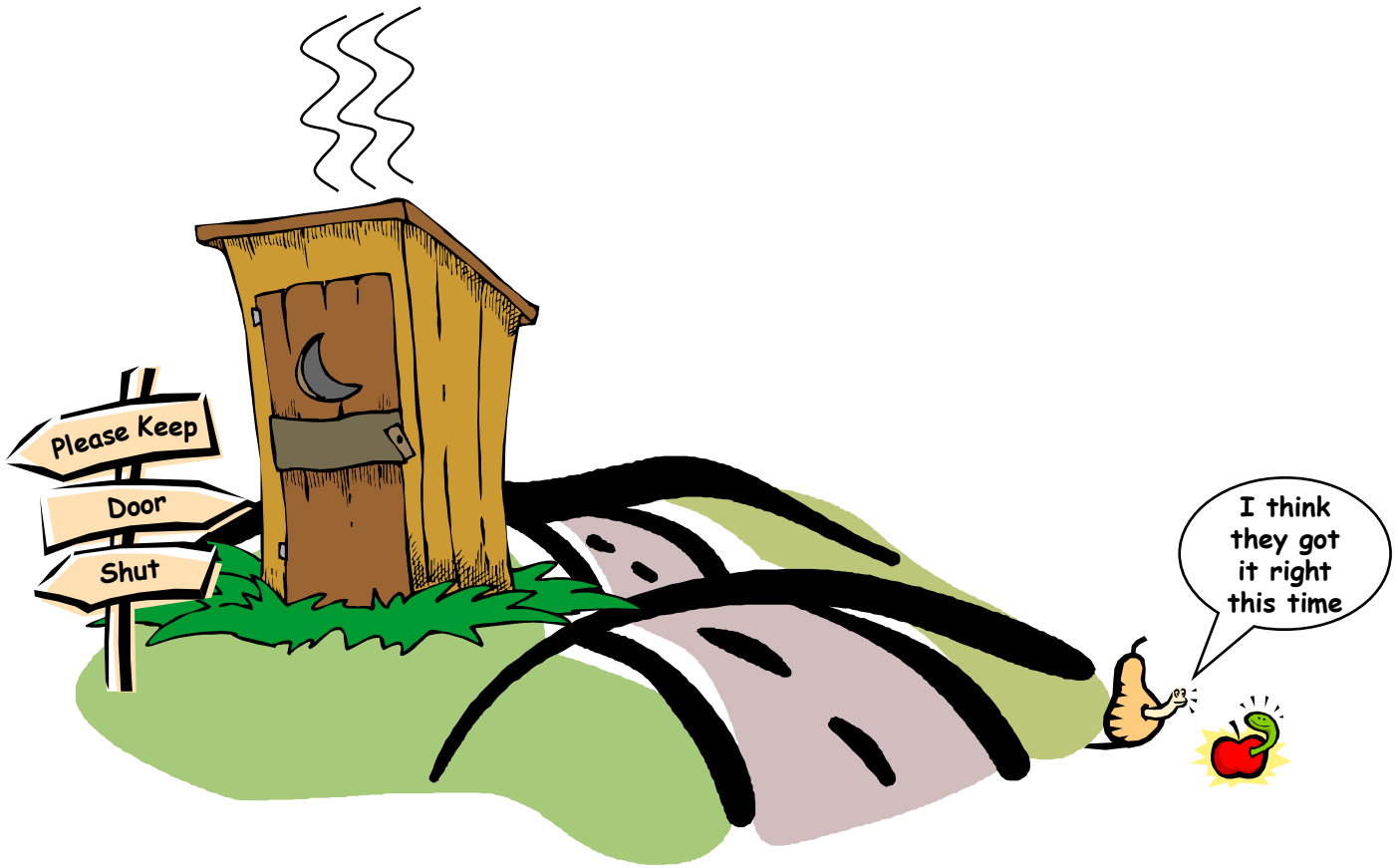
MITRE

Establishing Trust and Identification is Not in Itself a Security Solution

- Trust and identity may be necessary but are not sufficient to establish a secure relationship
- Identification does not indicate compliance of the source with respect to your security policies
- Trust says nothing about the competency of the source with respect to security policies
- Example: Accidental virus infection by trusted/identified individual
- All actions must be verified whether from trusted/identified source or not

MITRE

Conclusions

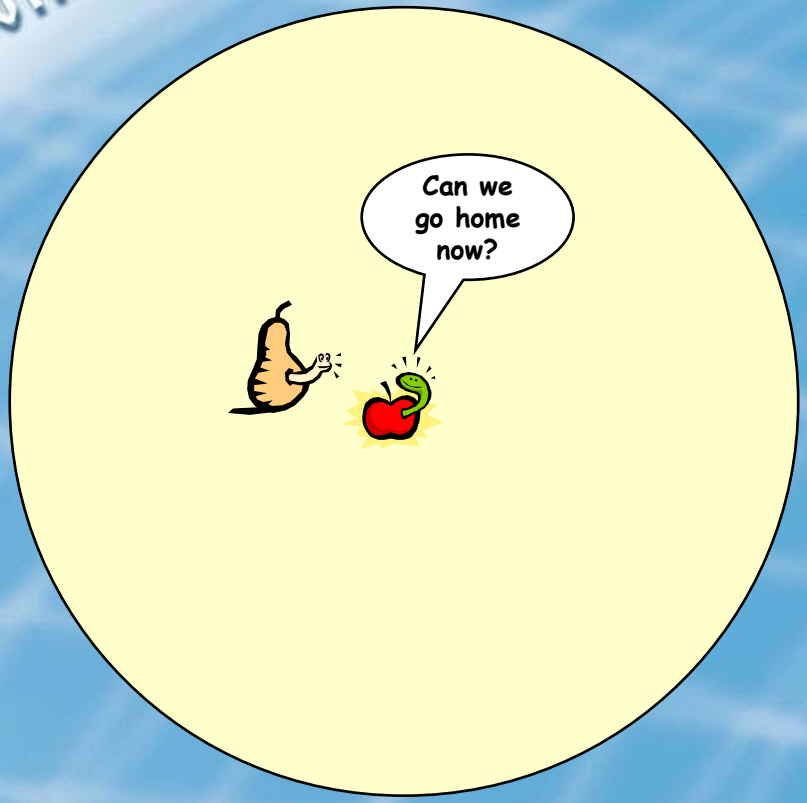


MITRE

Conclusions

- The aviation environment is different from that envisioned for COTS security tools
  - Rote application of security tools can lead to problems
  - One should be concerned with a security design/review by persons not aware of this difference
- Think security before, during, and after designing the aviation service/product
  - Otherwise expect to redesign the product when you address security
  - In many cases security is part of the infrastructure, not an addition to the infrastructure

CENTER FOR ADVANCED AVIATION SYSTEM DEVELOPMENT



MITRE